Private Industry Experience

How can small-to-mid sized companies cope with advanced, targeted attacks?

Andrew Klucsarits
CISO
The SI Organization, Inc.

thesiorg.com

CYBER SECURITY

the SI

Power of Integration

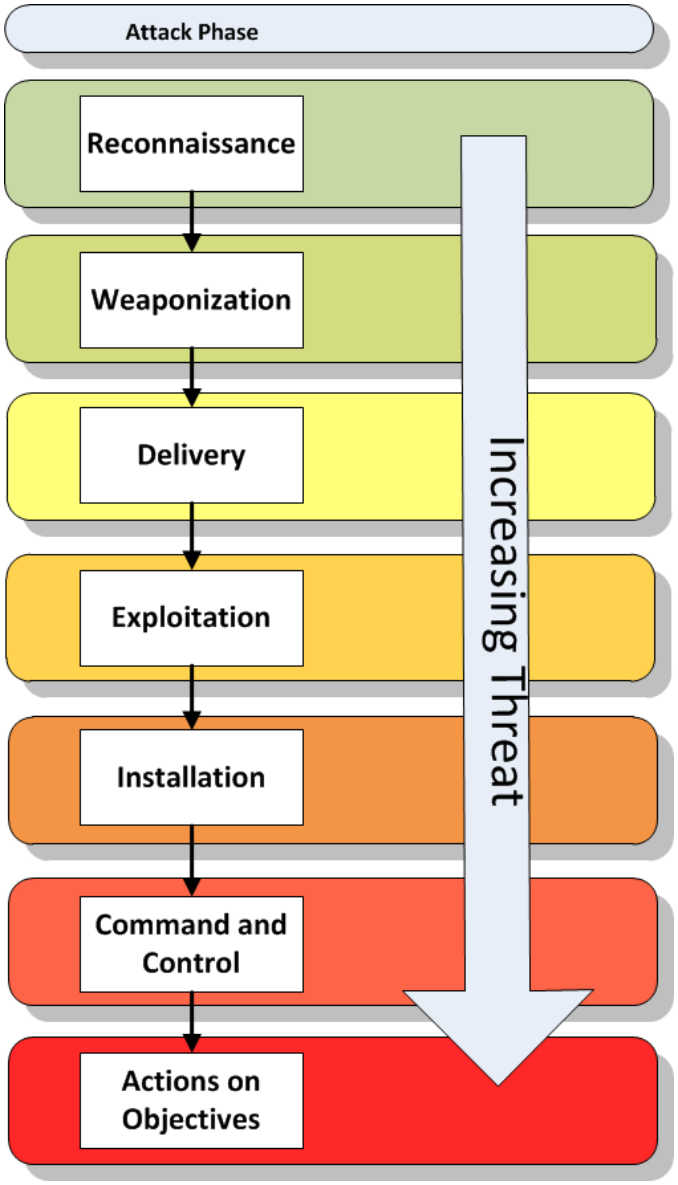
The SI Organization, Inc. Overview

- The SI Organization, Inc.
  - Approximately 2000 staff, including subsidiaries
  - Locations in VA, MD, PA, NJ, CO, CA, MO
  - Legacy of Lockheed Martin System Engineering and Integration and Bell Labs Research and Development
  - Mostly Federal DoD customers with a growing mix of commercial customers
    - Healthcare
    - Utility
    - Telecommunications

Cyber Defense

- The SI's Defense Strategy
  - Treat Incident Response holistically
    - Effective incident response begins long before the incident actually occurs
    - Right combination of people, process, and technology
      - Experienced staff trained in our response processes
      - Tools that provide both defense and visibility
  - Focus on disrupting the Cyber Kill Chain
    - Interrupt the attack as high in the chain as possible
    - Effective Threat Intelligence that delivers actionable intel
    - Smart investments in technology

Cyber Kill Chain



Visibility

Visibility into systems and data flows

Visibility

Visibility into the organization is crucial to detecting potential security incidents

- Access Management events
- Privileged access
- Data flows
- Unstructured data repositories
- Remote access
- Anomalous network traffic
- Endpoint computing devices
- Various system alerts

Visibility

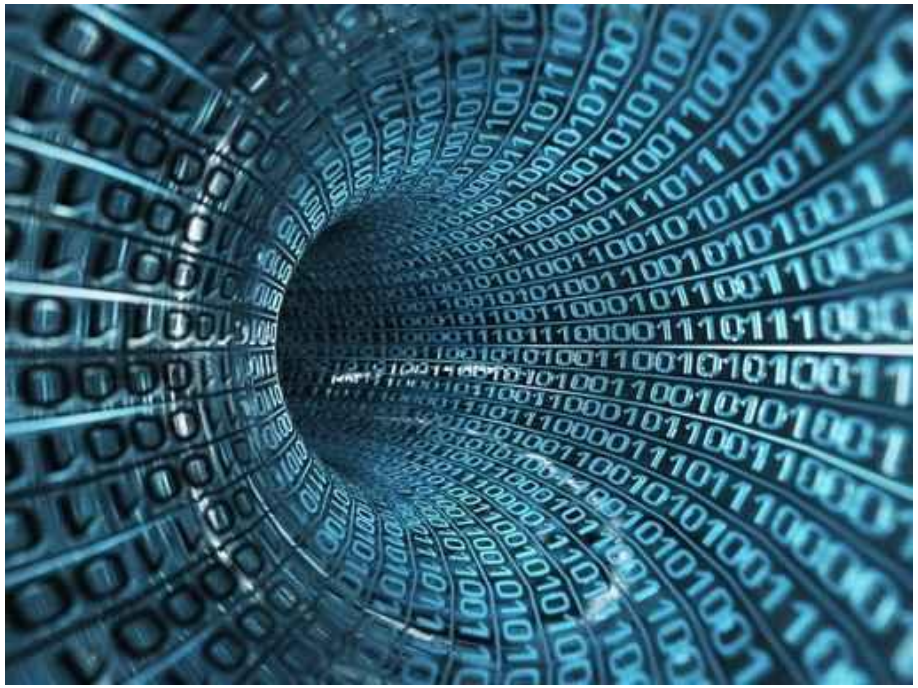
COTS and FOSS Products

- IDS/IPS
- Behavioral-based malware detection
- Endpoint protection
- Traditional firewalls
- Application-Aware (“Next Gen”) Firewalls
- SIEM
- Full Packet Capture
- SSL inspection
- Flow Data

Custom tools

- Incident Tracker
- File Identification and Alerting System (FIAS)
- Domain List (Indexed domain name search)
- IP List (Firewall log search)
- HitList (Alerting for monitored Domain and IP lists)

Self-Assessment



Continuous proactive self-assessment

Self-Assessment

Continuous proactive self-assessment

- Vulnerability Assessment
  - Network vulnerability assessment
  - Web application vulnerability assessment
  - Continuous monitoring of new Common Vulnerabilities and Exposures (CVEs)
- Risk assessment
  - Change management
  - New technologies
  - 3rd party service providers and partners

Threat Intelligence

Proactive Threat Intelligence

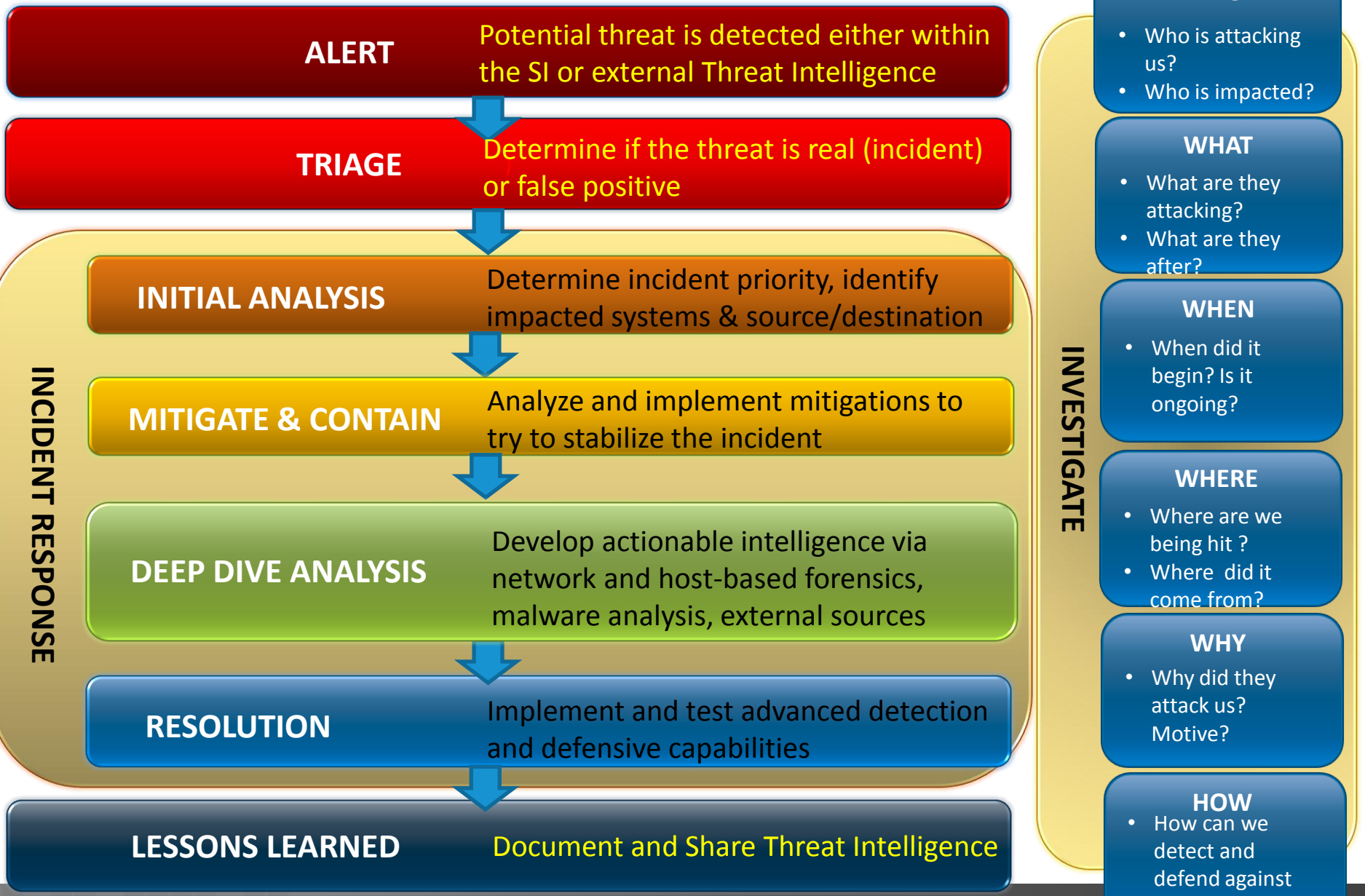
Threat Intelligence

- Government Sources
  - DSIE (defense security information exchange)
    - Collaboration effort between DHS (US-CERT)and Industry
  - DIB (defense industrial base)
    - Collaborative effort between US DoD and Industry
  - Infragard
    - Collaborative effort between FBI and Industry
- Direct Sources
  - Industry / peer network collaboration
  - SI Incident Response process
- Web
  - OS and Application vulnerabilities
  - Trends and changes in malware behaviors
  - Weaponization trends and Infection vectors
- Alerts on keywords and traffic trends
  - Twitter (tweetalarm)
  - Google Alerts
  - Google Analytics
  - Domain Tools

Incident Response

Incident Response People and Process

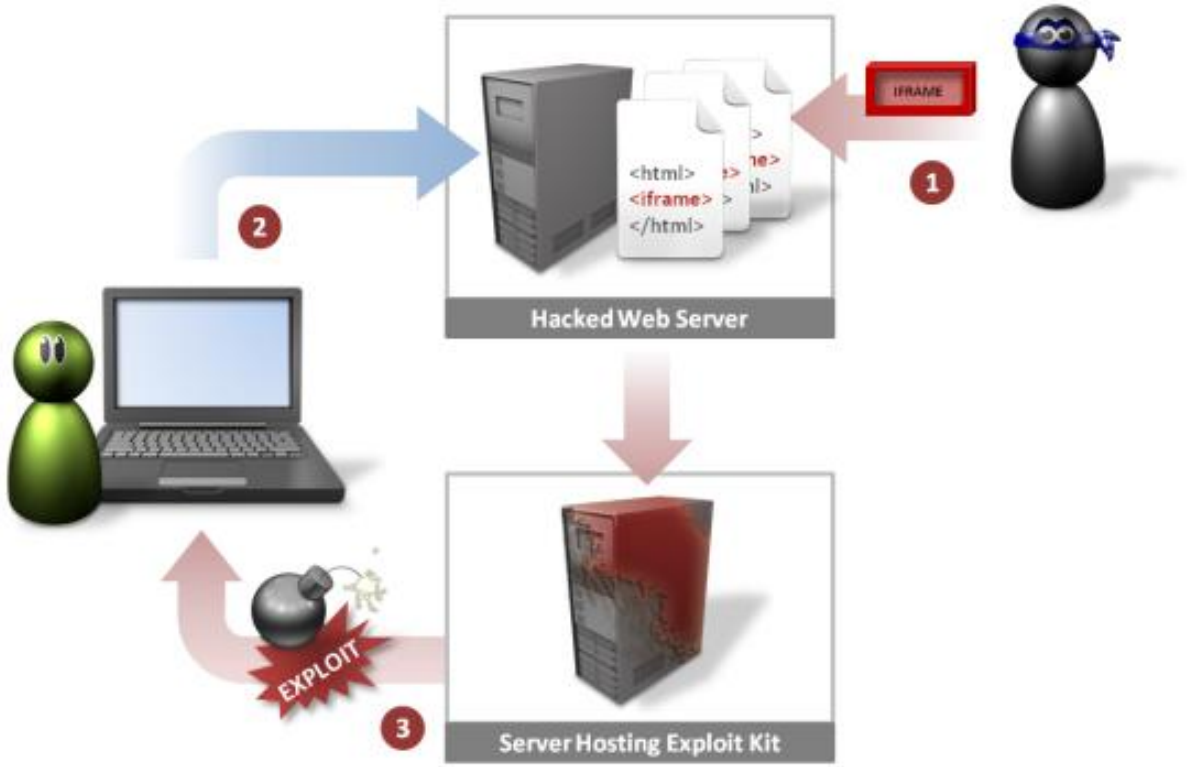
Incident Response Process Flow



Real World Examples

How does it work in the real world?

Water Hole Attack



Steps in Attack

1. Attacker hacks legitimate Web server and injects IFRAME into Web pages
2. User browses to legitimate Web site
3. Returned Web pages contain IFRAME pointing to server hosting exploit kit

IHS Water Hole Attack Defense [Part 1]

- IHS Global Insight
  - Financial research and forecasting services
  - Authorized SI user connected and logged in

- Incident identification, triage, and stabilization
  - Received alert from IDS that does behavioral analysis of downloaded executables
  - Validated the alert was probably real
  - Identified the affected computer
  - Found and pulled it from the network within 15 minutes
  - Block known command & control domains

IHS Water Hole Attack Defense [Part 2]

- Incident deep dive analysis, remediation, and resolution
  - Conduct forensic analysis on the affected workstation to acquire malware sample
  - Malware analysis (0-Day exploit)
  - Build detective and defensive capabilities
    - Yara signature to detect the specific malware variant
    - Signature to detect the type of attack (Java application attempting a download)
  - Conduct historical searches for other affected endpoints

Heartbleed Defense

- Heartbleed
  - OpenSSL module vulnerable to remotely exploitable stack overflow
  - Approach
    - Identify affected systems and services
      - Externally-facing
      - Externally-facing 3rd party
      - Internal
    - Patch
    - Revoke and replace affected SSL certificates
    - Deploy detections for exploit attempts
    - Monitor for campaigns

Respect | Accountability | Dedication | Improvement | Integrity

Back Up Slides

The SI Threat Operations Center

Enterprise-wide visibility

Actionable intelligence

Comprehensive analytical tools

Collaborative workspace

Rapid incident response

Pro-active responses to threats